ТЕХНИЧЕСКИЕ РЕШЕНИЯ, ПРИМЕНЯЕМЫЕ ДЛЯ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В СИСТЕМАХ КЛАССОВ 3А И 2А

С. В. Скурлаев, А. Н. Соколов
(Челябинск, ЮУрГУ (национальный исследовательский университет), cc@sbchel.ru)

Основные положения технической защиты информации изложены в специальном руководящем документе Гостехкомиссии России [1]. В нем определяются цели и направления технической защиты информации в автоматизированных системах (АС) от несанкционированного доступа (НСД), а также основные способы обеспечения защиты. НСД определяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или АС. Основные концептуальные положения раскрываются в других специальных нормативных актах: например, документом, описывающим классы АС, является [2]. В нем закрепляются три основных класса АС, каждый подразделяется на подклассы, к которым предъявляются определенные требования по реализации тех или иных механизмов. Для реализации последних можно применять средства защиты, отвечающие требованиям Гостехкомиссии и ФСТЭК.

Довольно распространенными АС являются системы 3-го и 2-го классов, в которых участвуют в обработке соответственно один или несколько пользователей, но обрабатываемая информация имеет одинаковый уровень ограничений к распространению. Среди средств защиты информации (СЗИ) чаще встречаются такие, которые отвечают требованиям для АС классов 1Г (обработка несекретной информации) или 1Б (обработка до «Совершенно секретно» включительно), так как требования на более низкие классы выполняются автоматически. Но сами СЗИ при этом весьма разнообразны. Подходы разработчиков к реализации одних механизмов защиты информации схожи, для других – отличны. Для выполнения определенных требований эти средства используют штатные функции операционных систем (ОС) семейства Microsoft Windows,

например, подсистему дискреционного разделения доступа. Для реализации других механизмов схожим остается только замысел. Соответственно для одних функций СЗИ сами предъявляют требования к системе, а для других используют свои драйвера и службы.

Задачей поставленного эксперимента является выяснение слабых и сильных сторон различных технических решений, применяемых для защиты от НСД. Для эксперимента были выбраны СЗИ, представленные в таблице. Критериями выбора являются: 1) доступность экземпляров СЗИ; 2) отличия в заявленных технологических подходах к реализации механизмов защиты. Эксперимент проводился при помощи программных продуктов Sysinternals: 1) Autoruns (отражает перечень драйверов, служб, модулей оболочки и входа в ОС и др.); 2) Process Explorer (показывает работающие процессы, а также их подчиненность, используемые файлы и директории); 3) Process Monitor (отслеживает действия всех процессов в системе, в том числе драйверов и библиотек, позволяет установить драйвер мониторинга с самого начала загрузки ОС). С помощью этих программ проанализированы устойчивость к сбоям и влияние механизмов СЗИ на запросы ПО к защищаемой информации:

1. Secret Net 6 имеет сертификат соответствия требованиям руководящих документов [3] (по 3-му классу защищенности) и [4] (по 2-му уровню). Применение данного средства возможно в подавляющем большинстве АС (до 1Б включительно). Например, для ограничения загрузки с внешних носителей требуется установить плату аппаратной поддержки или электронный замок «Соболь», предоставляющие возможность использования считывателей iButton. Для использования других аппаратных идентификаторов (eToken и Rutoken) достаточно наличия USB-портов на компьютере. Ограничением функционирования Secret Net 6 является требование к ОС (Windows от 2000 до 7 в версиях Professional), поскольку для управления средством требуются некоторые оснастки консоли.

Перечень компонент Secret Net 6 включает службу ядра, локальную базу данных системы защиты, подсистему регистрации и журнал Secret Net, подсистему локального управления, защитные подсистемы, модуль входа, подсистему контроля целостности, подсис-

Сравнение средств защиты информации

Средство защиты информации	Ядро СЗИ	Механизмы контроля доступа к файлам	Ограничение загрузки	Достоинства и недостатки
Secret Net 6	Служба и драйвер ОС	Реализованы как отдельные драйверы-фильтры ОС (запросы программ сравниваются с меткой сессии, объекта и разрешений пользователя)	Аппаратный модуль (или программный для АС класса 1В)	Слабым местом является служба ядра СЗИ, так как в случае ее отказа вход разрешается только администраторам. В случае отказа аппаратной части (хищения жесткого диска с программным модулем ограничения загрузки) возможна загрузка со сторонних носителей. Хорошая интегрируемость в ОС
Страж NT 3.0	Драйвер ядра ОС	Реализованы как отдельные драйверы-фильтры ОС	Сокрытие логической структуры диска	При контроле потоков не требуется выбирать уровень метки сессии, но значительно усложняется процесс настройки подсистемы мандатного доступа (для часто используемых программ есть шаблоны от производителя). В случае потери ключа преобразования загрузка ОС невозможна. Запросы программ перенаправляются механизмам СЗИ, поэтому для них логика их работы прозрачна, любая операция всегда завершается успешно, метка сессии не требуется. Широкий спектр поддерживаемых ОС
Аура	Отсутствует: служба ОС SKernel обслуживает только централизованную БД СЗИ	Реализованы как отдельные драйверы-фильтры ОС (запросы программ сравниваются с меткой сессии, объекта и разрешений пользователя), а также ряд служб, осуществляющих служебные операции	Прозрачное преобразование (кодирование) дисков	В случае отказа службы ядра СЗИ продолжает функционировать. В случае потери ключа шифрования загрузка ОС невозможна. Узкий перечень совместимых ОС

тему работы с аппаратной поддержкой, а также криптоядро, которое производитель не выделяет в отдельную компоненту ввиду использования несертифицированных алгоритмов. Часть механизмов, включая ядро Secret Net 6, работают как службы ОС. В случае отказа одной из служб перестают выполняться связанные с ней механизмы, отказ службы ядра может привести к неработоспособности СЗИ в целом, позволяя зайти в систему только с административными правами. В случае использования в АС третьего класса единственный пользователь будет иметь такие полномочия. В общем случае средство защиты расширяет возможности ОС, внедряя драйверы-фильтры в необходимых моментах: файловые операции, обращения к устройствам, вход-выход и другие действия пользователей. Настройки СЗИ хранятся в реестре и некоторых файлах; при их повреждении не всегда остается возможной корректная деинсталляция средства защиты.

2. Страж NT 3.0 имеет сертификат соответствия требованиям руководящих документов [3] (по 3-му классу защищенности) и [4] (по 2-му уровню). Ограничения загрузки с других носителей реализуются через сокрытие логической структуры диска. В качестве идентификаторов используются: гибкие магнитные диски, iButton, eToken, Rutoken и Guardant ID. Функционирует в любых версиях ОС Windows от 2000 до 7.

Страж NT 3.0 имеет следующие модули [5]: модуль входа в систему, модуль загрузки, модуль ядра системы защиты, службу доступа к устройствам, подсистемы защиты. Ядро рассматриваемого СЗИ реализовано как драйвер ядра ОС, поэтому отпадает вариант дестабилизации средства защиты из-за неработающей службы. Поскольку Страж NT 3.0 при использовании модуля входа в систему обеспечивает сокрытие логической структуры диска, то слабым местом остается носитель-идентификатор: в случае его утраты или неработоспособности вход в систему невозможен. Необходимо отметить, что само СЗИ при этом позволяет сделать дубликат идентификатора. Для разделения доступа также используются драйверы-фильтры, которые перенаправляют запросы в случае обращений к файлам и устройствам внутренних механизмов СЗИ. Благодаря такому

подходу Страж NT 3.0 является толерантным в отношении ОС, под которой он будет работать.

3. Аура имеет сертификат соответствия требованиям руководящих документов [3] (по 3-му классу защищенности) и [4] (по 2-му уровню). Ограничения загрузки со сторонних носителей реализованы путем прозрачного преобразования дисков с помощью патентованных методов. В качестве аппаратных идентификаторов может применяться Rutoken, а при использовании электронного замка «Соболь» – iButton. Перечень ОС, поддерживаемых рассматриваемым СЗИ, ограничен (Microsoft Windows 2000 Professional SP4, 2000 Server SP4, XP Professional SP3, Server 2003 Standard Edition SP2, Server 2003 Enterprise Edition SP2, Server 2008 Standard Edition SP2, Server 2008 Enterprise Edition SP2, Vista Business SP2, Vista Ultimate SP2).

Аура имеет множество модулей, реализованных как в качестве службы, так и в качестве драйверов системы и библиотек оболочки. Особенностью СЗИ является механизм контроля целостности и редактирования базы данных пользователей (включая их полномочия) до загрузки ОС. Как и в случае с Secret Net 6, СЗИ поддерживает несертифицированное шифрование, но обладает способностью полностью преобразовывать диски, включая виртуальные, инструменты для создания которых имеются в самом средстве. На данный момент слабым местом средства защиты информации является не очень широкий перечень поддерживаемых ОС.

Таким образом, все СЗИ обладают как достоинствами, так и недостатками, наличие которых определяется используемыми технологиями и конкретными реализациями. Выбор того или иного СЗИ должен определяться степенью риска потерять защищаемые носители или идентификаторы, утратить защищаемые данные во внештатных ситуациях.

Библиографические ссылки

1. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации: утв. решением Гос. техн. комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс]. Режим доступа: http://

fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (дата обращения: 10.10.2013).

2. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации : утв. решением председателя Гос. техн. комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс]. Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (дата обращения: 10.10.2013).

3. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации : утв. решением председателя Гос. техн. комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс]. Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (дата обращения: 10.10.2013).

4. Защита от несанкционированного доступа к информации. Ч. 1: Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей: утв. решением председателя Гос. техн. комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114. [Электронный ресурс]. Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty (дата обращения: 10.10.2013).

5. Система защиты информации от несанкционированного доступа «СТРАЖ NT» Версия 3.0. Описание применения. 2010 г. [Электронный ресурс]. Режим доступа: http://guardnt.ru/download/doc/app_guide_nt_3_0.pdf (дата обращения: 10.10.2013).

РАЗВИТИЕ MESH-СЕТЕЙ С ПОМОЩЬЮ МОБИЛЬНЫХ УСТРОЙСТВ

Н. А. Токарчук, А. Н. Соколов
(Челябинск, ЮУрГУ (национальный исследовательский университет), conference+urfu@mainnika.ru)

Современные глобальные компьютерные сети, несмотря на все свои преимущества, имеют существенный недостаток – они централизованы. Если выключается один узел связи – все те, кто был через него подключен, теряют связь. Общество сегодня слишком зави-